national policies.[31] Thus, in order that CALEA implementation not impair the carefully crafted framework for regulatory parity among the commercial mobile radio services, costs for CALEA compliance should not fall disproportionately on substantially similar commercial mobile radio services. If disparities in CALEA cost burdens are permitted, competition between the services will be less vigorous.

Factor (J): Design and Development of the Equipment, Facility, or Service Initiated Before January 1, 1995

If equipment, facilities or services were commercially available on or before January 1, 1995, the Commission should not require carriers to retrofit that equipment at carrier expense. It was not the intent of CALEA to make whole classes of service or switches obsolete.

The FBI has adopted a very narrow definition of "installed or deployed" in its Final Rule for cost reimbursement that restricts eligibility to equipment, facilities and services "operable and available for use" by each carrier's customers as of January 1, 1995.[32] Thus, the FBI rule would impose costs on carriers to upgrade any switch

---

[31] House Report at 3494.

[32] The Final Rules are set forth at 28 C.F.R. §§ 100.9-100.21. The FBI's definition is plainly arbitrary and capricious and the Commission should give no deference to it under this factor.

even if the platform model was under production at the time of CALEA, under contract for purchase by the carrier before January 1, 1995, and even deployed elsewhere in the carrier's network. In each of these circumstances, the Commission should grant carrier petitions to avoid undue hardship or expense.

Factor (K): Other Factors the Commission Determines Are Appropriate

Carriers should always be permitted to present other unique circumstances that make CALEA compliance unreasonably difficult. This is consistent with the Commission's policy of permitting waivers of Commission rules in appropriate circumstances where application of a rule is inequitable, unduly burdensome or contrary to the public interest or the underlying purpose of the rule would not be served or would be frustrated.[33]

3. FBI Participation Must Be on the Record

Congress intended that the FBI would be treated essentially as any other interested party in the Section 109(b) petition process. Unlike Section 107(c), which provides for consultation with the FBI in the determination of whether a carrier should be granted an extension for compliance, Section 109(b) provides only that *notice* of a

---

[33] See, e.g., 47 C.F.R. § 22.119(a).

petition be given to the FBI prior to the Commission making its determination. Section 109 does not provide for any special advisory or consultative role in the reasonably achievable determination.[34] Therefore, all participation by the FBI in these determinations must be disclosed in the public record and petitioners must have the opportunity to respond to any issues raised in FBI communications to the Commission. The FBI must also be subject to the Commission ex parte rules. Subjecting the FBI participation to public disclosure requirements will preserve the balance between the three interests to be considered in these proceedings: industry, privacy and law enforcement.

4. Filing a Petition Should Toll the Compliance Deadline

The Commission should automatically toll the compliance deadline upon the filing of a petition for a determination of whether compliance is reasonably achievable. Of course, such petitions may come after the compliance deadline, in which case the Commission should set the terms and conditions of carrier assistance pending a determination.

C. DEFINITION OF TELECOMMUNICATIONS CARRIER

CTIA agrees with the Commission that the definitions of the Communications Act of 1996 did not alter or amend the

---

[34] 47 U.S.C. § 1008(b).

definitions used in CALEA. Moreover, it is important to make clear that all classes of telecommunications carriers are covered if they offer telecommunications services to the public for hire and provide the subscriber with the ability to originate, terminate or direct communications.[35] This will ensure parity and fair treatment of all carriers.

Second, throughout the House Report accompanying the legislation, Congress emphasized that the capability requirements apply only to those services that enable the subscriber to make, receive or direct calls and do not apply to any information services such as email, voice mail or other on-line services.[36] Indeed, Section 102(8) of CALEA explicitly excludes persons and entities engaging in providing information services from the definition of telecommunications carrier[37] and Section 103(b)(2) of CALEA explicitly excludes information services from the Section 103 requirements.[38]

Information services provided by common carriers should not be treated any differently from those of other information services. Congress deliberately excluded all information

---

[35] House Report at 3498.

[36] See, e.g., House Report at 3498 ("Excluded from coverage are all information services").

[37] 47 U.S.C. § 1001(8).

[38] 47 U.S.C. § 1002(b)(2).

services from CALEA requirements because of regulatory burdens that might hinder the development of new technologies.[39] Wireless carriers and support service providers will continue to develop unique wireless information service applications. The Commission need only think of the remarkable new information services that have become available to the public in recent months in conjunction with their wireless handsets. The public interest would not be served by stifling what is at the moment the most exciting and dynamic component of the wireless services industry by imposing CALEA obligations on some carriers that provide information services but not on pure information service providers.

D. SYSTEMS SECURITY AND INTEGRITY

CTIA is surprised by the direction of the Commission with the proposed security rules for carriers. CALEA amended Title II of the Communications Act of 1934 in order to authorize the Commission to enact rules to implement Section 105 of CALEA, the systems security and integrity provision.[40] Section 105 provides:

> A telecommunications carrier shall ensure that

---

[39] House Report at 3501 ("It is the Committee's intention not to limit the definition of 'information services' to such current services, but rather to anticipate the rapid development of advanced software and to include such software services in the definition of 'information services.'").

[40] 47 U.S.C. § 229.

> any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.[41]

The intent of Congress was to prevent law enforcement from remotely activating wiretaps in the carrier's switching plant.[42] Section 105 does not deal with local loop interceptions or any law enforcement activity off-premises, nor does CALEA require that interceptions be switched-based.[43] Thus, CTIA is perplexed by the Commission's apparent focus on carrier employees and internal policies to limit knowledge about wiretap activity.[44]

---

[41] 47 U.S.C. § 1004.

[42] House Report at 3506.

[43] See House Report at 3506 ("Activation of interception orders or authorizations originating in local loop wiring or cabling can be effected by government personnel or by individuals designated by the telecommunications carrier, depending upon the amount of assistance required."). The Commission probably did not mean it literally when it said in the NPRM that Section 105 "requires a telecommunications carrier to enable the interception of communications content or access to call-identifying information via its switching premises." NPRM at ¶ 21. Obviously, local loop interceptions can and will continue without the affirmative intervention of carrier personnel.

[44] CTIA also is astonished by the FBI's apparent desire to force background checks on any carrier personnel involved in wiretapping. While the Commission apparently decided not to seek comment on the FBI proposal contained in the Worrell letter, the Commission still would require disclosure of

The procedures adopted under Section 229 should be minimal and should require only that carriers have policies to ensure lawful authorization is required before wiretaps will be executed. CTIA does not agree that Section 229 refers to internal carrier authorization as opposed to the actual court order served on the carrier.[45] Section 229 no doubt was intended to ensure that carriers received the *proper* authorization to respond to government demands, especially in light of the changes made by CALEA in the form of authorization.[46]

The Commission should not impose unduly restrictive recordkeeping obligations on carriers. It should be sufficient to meet the "secure and accurate" records requirements of Section 229 to require carriers to maintain the confidentiality of such documents. As a matter of prudent security practice, CTIA understands that most if not all carriers secure records related to interception activity under lock and key.

---

employee personal information such as date and place of birth and social security number to the FBI or other law enforcement agencies -- information that would be used for only one purpose -- background checks. CTIA urges the Commission to strongly reject this intrusion.

[45] NPRM, ¶ 29.

[46] See, e.g., 18 U.S.C. § 2703(d) as amended by CALEA Section 207(a).

Finally, if the Commission is satisfied that a certification process from small carriers that they meet the requirements of Section 229 satisfies the submission requirements of Section 229(b)(3), CTIA sees no reason not to require only the same from large carriers.[47] The Commission could reserve the right in its rules to request such procedures for review.[48]

---

[47] NPRM, ¶¶ 34-36.

[48] CTIA notes that it cannot be in the best interests of either law enforcement or carrier security to require filing such procedures on the open docket with the Commission where any person might obtain a copy.

III.
CONCLUSION

CTIA urges the Commission to squarely address the extension issue as soon as possible. The Commission has the opportunity to help implement CALEA cost-efficiently and as soon as practicable, just as Congress intended. The Commission should use its rulemaking powers under CALEA to ensure that procedures will be adopted as soon as possible to consider petitions for relief, where appropriate, from CALEA's capability requirements. CTIA is committed to all efforts to implement CALEA fairly and evenly across the industry.

Respectfully Submitted,

Michael Altschul
Vice President and
General Counsel

Randall S. Coleman
Vice President,
Regulatory Policy & Law

CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1250 Connecticut Ave., N.W.
Suite 200
Washington, D.C. 20036

December 12, 1997

TAB A

TELECOMMUNICATIONS®
TIA
INDUSTRY ASSOCIATION

CONTACT: **SHARON GRACE (TIA)**
(703) 907-7721
Sally Mott Freeman (ATIS)
(202) 434-8850

FOR IMMEDIATE RELEASE
December 5, 1997

TIA AND ATIS PUBLISH LAWFULLY AUTHORIZED ELECTRONIC SURVEILLANCE INDUSTRY STANDARD

Arlington, VA.-- The Telecommunications Industry Association and Committee T1, sponsored by the Alliance for Telecommunications Industry Solutions (ATIS), have jointly published interim standard/trial use standard J-STD-025, *Lawfully Authorized Electronic Surveillance*.

The purpose of this industry standard is to facilitate a telecommunication service provider's compliance with the assistance capability requirements defined in Section 103 of the Communications Assistance for Law Enforcement Act (CALEA) of 1994. An industry ballot unanimously approved this document as fulfilling the requirements called for under CALEA.

J-STD-025 defines the services and features to support lawfully authorized electronic surveillance and the interfaces to deliver intercepted communications and call-identifying information to a law enforcement agency when authorized.

Compliance with J-STD-025 satisfies the "safe harbor" provisions of Section 107 of CALEA and helps ensure efficient and industry-wide implementation of the assistance capability requirements.

The U.S. Congress, under CALEA, encouraged industry standards-setting bodies to establish standards to meet the lawfully authorized surveillance capabilities required by CALEA. Work began in early 1995 to develop a standard in TIA's engineering committee TR-45.2, Cellular Inter-System Operations, in conjunction with Committee T1. TIA's standards-setting

-more-

process invites participation of all interested parties, and industry participants as well as government representatives made technical contributions to be considered for text in the standard.

The formulating group, made up of industry representatives, unanimously approved J-STD-025 for publication as a joint TIA interim standard/Committee T1 trial use standard. By definition, an interim standard contains information deemed to be of technical value to the industry and must be reviewed on an annual basis with consideration to proceed to develop an American National Standard on the subject.

To obtain a copy of J-STD-025, contact Global Engineering Documents at (800) 854-7179 or at *http://global.ihs.com*.

###

TIA is a full-service national trade organization with membership of 650 large and small companies which provide communications and information technology products, materials, systems, distribution services and professional services in the United States and countries around the world. TIA represents the telecommunications industry in association with the Electronic Industries Association.

Nearly 2,500 experts from 500 companies participate in ATIS committees, whose work ranges from developing United States network interconnection standards to operating guidelines for network testing. The FCC frequently refers operations issues to ATIS committees for recommended solutions. ATIS membership is open to North American and World Zone 1 Caribbean providers of telecommunications services as well as providers engaged in the resale of those services; all manufacturers of telecommunications equipment and developers of telecommunications software for such equipment used for the provision of telecommunications services and all providers of enhanced services.

EDITORS: Please note that information regarding TIA and ATIS is available via the associations' respective World Wide Web site at *http://www.tiaonline.org and http://www.atis.org.*

P.A. Release 97-96
12.5.97

TAB B

Building The Wireless Future.

CTIA

Cellular
Telecommunications
Industry Association
1250 Connecticut
Avenue, N.W.
Suite 200
Washington, D.C. 20036
202-785-0081 Telephone
202-466-7239 Fax
202-736-3221 Direct Dia

Arthur L. Prest
Vice President for
Science and Technology

November 20, 1997

Mr. Dan Bart
Vice-President, Standards and Technology
Telecommunications Industry Association
2500 Wilson Boulevard, Suite 300
Arlington, Virginia 22201-3834

Re: CTIA Recommendation to Publish SP-3580A as ANSI Standard

Dear Dan:

On November 19, 1997, the Cellular Telecommunications Industry Association ("CTIA") urged the TR45.2 Subcommittee to recommend publication of SP-3580A as an American National Standards Institute ("ANSI") standard. The Subcommittee agreed with CTIA's recommendation and forwarded their recommendation to you. CTIA sends this letter to explain the basis for its recommendation, especially in light of law enforcement's objection to publication of the proposed industry standard, and to urge TIA to act as soon as possible on the recommendation.

I. RATIONALE FOR ANSI STANDARD

The TR45.2 Subcommittee decided long ago that it would seek ANSI approval for then PN-3580 to meet the Section 107 "safe harbor" provisions of the Communications Assistance for Law Enforcement Act ("CALEA"), which requires that technical standards be publicly available and adopted by an industry association or standard setting organization. Law enforcement has objected to publishing the standard without certain additional capabilities that it believes are required by CALEA but which have been rejected by the industry as outside of CALEA entirely.

There are at least three reasons to publish an ANSI standard notwithstanding law enforcement's ballots to the contrary. First, law enforcement's authority in the standards setting process is limited by law to "consultation." They are not entitled to

dictate a specific design or any functional requirements; and conversely, they are not entitled to block or prevent the deployment of any CALEA solution by carriers and manufacturers. Even though the Telecommunications Industry Association ("TIA") rules permits any interested party to participate in the ANSI standards process and therefore to vote on a proposed standard, law enforcement cannot use the TIA standards process to do what CALEA otherwise prohibits.[1]

Second, law enforcement's comments on the SP-3580A ballot had been considered previously by the Subcommittee and rejected as seeking capabilities that were beyond the scope of CALEA. Thus, law enforcement's comments were not technical, but rather related to legal interpretations of the scope of CALEA. While law enforcement contends that the absence of its desired list of capabilities makes the proposed industry standard deficient, the Subcommittee is not the proper forum to resolve that complaint. Congress expressly provided that the Federal Communications Commission ("FCC") would be the venue for determining whether a standard meets the Section 103 capability assistance requirements. In sum, the nontechnical legal objections of law enforcement should be treated by TIA as not responsive and disregarded.

Third, qualitatively, even if the ballot responses were relevant and law enforcement was entitled to use the standards process to force additional capabilities into the standard, the ballot responses should be rejected as uninformed and the product of apparently misleading information. The ballot comments predominantly were crafted by the Federal Bureau of Investigation ("FBI") and joined in by local agencies. In fact, the FBI submitted substantially all of the ballots under its own cover letter.

Through two ballot cycles, law enforcement has generated substantial "no" votes from federal, state and local law enforcement agencies in an apparent attempt to

---

[1] Perhaps recognizing the improper use of the TIA voting process, a senior FBI official testified in an October 23, 1997, hearing before the House Subcommittee on Crime, under oath that law enforcement was not "voting" in the process, only offering comments. Steve Buyer R/IN, member of the House Judiciary Committee, questioned why industry had been detained by law enforcement's "comments" at all and that it was not the intent of Congress that the development of an industry standard, to be a safe harbor, require law enforcement's participation or voting at all.

block the proposed standard from going forward.[2] A close review of the ballot comments discloses that virtually none of the law enforcement voting parties were participants in the standards setting process; they had never attended a standards meeting; they probably never read the standard and were relying on mischaracterizations of the standard and the directions of certain law enforcement participants in the process to cast their ballots.

For example, almost half of the no votes on the second ballot were received from local law enforcement agencies in Wisconsin, a state not known for its electronic surveillance needs and not even one of the areas identified by law enforcement in the past as a high priority area for receiving CALEA support. It is not clear what these nonparticipants in the standards meetings were told in the solicitation of their votes, but it is clear that they were not told what the standard does provide. In fact, one of the Wisconsin commenters apparently believes the standard is about charging law enforcement for copies of customer transaction records in the future. Other votes from local law enforcement equally were without substance or understanding.

In short, law enforcement's "no" votes are not permitted under CALEA and in any event they are not responsive to the technical standards document.

II. LEGAL RATIONALE

Congress made crystal clear that the telecommunications industry sets the standard for implementation of CALEA's capability requirements. In the House Report accompanying the legislation, Congress stated that Section 107 "establishes a

---

[2] CTIA notes that if TIA or ANSI considers law enforcement's "no" votes, they may need to consider whether there is a dominance issue given the size of the law enforcement community as an interest category. Also, TIA or ANSI could consider law enforcement's votes as a only one vote given that the Communications Industry Section, formerly known as the Telecommunications Industry Liaison Unit and the Telecommunications Contract and Audit Unit, is comprised of federal, state and local law enforcement representatives and represents all law enforcement interests in CALEA.

mechanism for implementation of the capability requirements that defers, in the first instance, to industry standards organizations.[3]

Congress was persuaded that it was necessary to delegate the standard-setting role to the industry rather than the Attorney General in order not to chill technological innovation and to allow industry to fulfill its obligations in the most cost-efficient manner for industry. This act of Congressional delegation underscores that industry has the exclusive role in drafting the standards and that law enforcement does not have the authority to define the requirements necessary to implement Section 103.

First, Congress noted that the use of standards to implement legislative requirements is appropriate so long as Congress delineates the policy that the guidelines must meet.[4] In the case of Section 103, Congress noted that the four Section 103 requirements provided much more specificity than found in many delegations. Thus, a standards setting body would have no special difficulty in meeting the goals of Congress through standards.

Second, and most important, Congress stated "[t]he authority to issue standards to implement legislation delegated here to private parties is well within what has been upheld."[5] It especially was appropriate to delegate authority to implement Section 103 through standards to private parties, here the telecommunications industry,[6] because the resulting standards would be voluntary and "the FCC retains control over the standards."[7]

---

[3] H. Rep. No. 103-827, at 26 (1994), *reprinted in* U.S.C.C.A.N. 3489, 3506 (emphasis added).

[4] Id. (citing Skinner v. Mid-America Pipeline Co., 490 U.S. 212, 220 (1989)).

[5] Id. at 27 (emphasis added).

[6] Congress understood, of course, that the telecommunications industry had a long history of cooperating with law enforcement in the conduct of lawfully authorized electronic surveillance. While law enforcement may be the user of community for surveillance features, they have no monopoly on understanding the surveillance requirements because the telecommunications industry itself has been at the forefront of providing technical assistance for implementing wiretaps.

[7] Id.

What this legislative history makes perfectly clear is that in delegating authority to set the safe harbor standard to industry, Congress meant to preclude law enforcement from requiring private parties to adhere to a standard law enforcement might attempt to mandate[8] and that it is the FCC, not law enforcement, that has control over the content of any standard. This is no doubt the case because Congress previously had rejected law enforcement's preferred legislation that would have granted the right to the Attorney General to set the technical standards in the first instance.[9]

Thus, Congress stated in the clearest of terms:

> The legislation provides that the *telecommunications industry itself* shall decide how to implement law enforcement's requirements. The bill allows industry associations and standard-setting bodies, in consultation with law enforcement, to establish publicly available specifications creating "safe harbors" for carriers. This means that those whose competitive future depends on innovation will have a key role in interpreting the legislated requirements and finding ways to meet them

---

[8] Id. ("the FCC. . . has the authority to reject the standards developed by industry and substitute its own.") An original co-sponsor of CALEA, Congressman Hyde, noted that the delegation to industry was a negotiated "trade-off" given that industry was to bear the expense of compliance after the four year transition period. See 140 Cong. Rec. 10771, 10799 (Oct. 4, 1994) (comments by Rep. Hyde); *see also id.* at 10780 (comments by Rep. Markey), 10782 (comments by Rep. Edwards).

[9] See, e.g., Joint Hearing of the Technology and Law Subcommittee of the Senate Judiciary Committee and the Civil and Constitutional Rights Subcommittee of the House Judiciary Committee (Federal News Service, Mar. 18, 1994):

> Senator Leahy: So what you're saying is that you want this committee to set an industry-wide, uniform standard, which may not be the standard the industry wants and may be [sic] legislatively impeding technological advances that would be there without our stepping in?
>
> FBI Director Freeh: Yes. Yes, we want this committee to set and mandate requirements in future equipment, which is currently being engineered and deployed. . . .

> without impeding the deployment of new services. If industry associations or standard-setting organizations fail to issue standards to implement the capability requirements, or if a government agency or any person, including a carrier, believes that such requirements or standards are deficient, the agency or person may petition the FCC to establish technical requirements or standards.[10]

Thus, the proper role for law enforcement under CALEA is not to dictate standards at all. Rather, Section 107(a)(1) provides that the Attorney General[11] in coordination with other law enforcement agencies shall consult with the telecommunications industry, users of telecommunications equipment, and state utility commissions to ensure an efficient and industry-wide implementation of the assistance capability requirements.[12] Consultation does not include setting the standard, preventing the standard from being published, or negotiating to include capabilities in the industry under the threat of future enforcement actions.

Accordingly, under Section 107(b), law enforcement's exclusive forum to raise any claims that the industry standard is "deficient" or otherwise fails to provide the required assistance capability is the FCC.

---

[10] H. Rep. No. 103-827, at 19 (1994), *reprinted in* U.S.C.C.A.N. 3489, 3499.

[11] The Attorney General has delegated her role to the FBI. See Federal Bureau of Investigations--General Functions [AG Order No. 1951-95], 60 Fed. Reg. 11906 (Dep't Justice 1995) (codified at 28 C.F.R. pt. 0).

[12] CALEA Section 107(a) provides:

> (1) **Consultation.** To ensure the efficient and industry-wide implementation of the assistance capability requirements under section 103, the Attorney General, in coordination with other Federal, state, and local law enforcement agencies, shall consult with appropriate associations and standard-setting organizations of the telecommunications industry, with representative of users of telecommunications equipment, facilities, and services, and with State utility commissions.

III. CONCLUSION

For all of the reasons above, CTIA urged the Subcommittee to recommend publication of SP-3580A as an ANSI standard. Law enforcement is not entitled by law to thwart industry standards setting efforts and so cannot be empowered by TIA rules to do so by exercising a de facto veto over industry proposals simply by generating the most "no" votes.

CTIA notes that it also recommended, and the Subcommittee agreed, to publish PN-4116 as Joint TIA Interim Standard and T1 Trial Use Standard, J-STD-025. If the recommendation to publish the ANSI standard is approved, CTIA recommended, and the Subcommittee agreed, that J-STD-025 should be rescinded and replaced with what would be ANSI standard J-STD-025A.

CTIA appreciates TIA's consideration of this letter and urges that TIA act as soon as possible on this recommendation.

Sincerely

TAB C

Building The Wireless Future

CTIA
Cellular Telecommunications Industry Association
1250 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20036
202-785-0081 Telephone
202-331-8112 Fax
202-736-3213 Direct Dial

Thomas E. Wheeler
President / CEO

November 12, 1997

Mr. Stephen R. Colgate
Assistant Attorney General
for Administration
Department of Justice
950 Pennsylvania Ave NW
Room 1111
Washington, D.C. 20530

Re: Moving Forward on CALEA

Dear Steve:

As I mentioned in our last conversation, the Cellular Telecommunications Industry Association ("CTIA") wants to help Department of Justice meet Chairman Rogers' injunction to reach agreement on implementation of the Communications Assistance for Law Enforcement Act ("CALEA") by January 4, 1998. This letter sets forth our plan for achieving Chairman Rogers' goal in the context of the issues discussed at Chairman McCollum's hearing -- the four "Cs" of capability, compliance date extension, cost recovery and capacity.

First, on capability, CTIA will ask the industry standards committee next week, upon resolution of any remaining ballot comments, to recommend to the Telecommunications Industry Association ("TIA") that SP-3580A be published immediately as an American National Standards Institute ("ANSI") standard. The fact that the committee rejected law enforcement's ballot comments that urged additional capabilities be included in the standard, should not stop the industry standard from going forward to ANSI for immediate publication. Law enforcement has no technical issues with the industry standard, only disagreement over the scope of CALEA; and, promulgation of the standard in its proposed form will not preclude the addition of other advanced features in the future. We hope the Department of Justice will support publication of an ANSI standard at next week's TIA meeting. Carriers and manufacturers want to get on with bringing the significant capabilities contained in the PN-3580A to the street.

Coupled with promulgation of the ANSI standard now, CTIA will propose to TIA that it initiate a new standards project to be called "Enhanced Electronic Surveillance Services." The project will deal with the standardization of the advanced surveillance features requested by law enforcement on the so-called FBI punch list, where technically feasible and lawful. Once standardized, law enforcement would be free to order these service capabilities on an a la carte basis from manufacturers. Law enforcement could then direct development funds to manufacturers, licensing the final features package to carriers at no cost and on an as needed basis.

Taken together, this standardization effort -- SP-3580A now and the Enhanced Electronic Surveillance Services standard in progress -- should solve the capability issue. Of course, we would need to jointly agree on an extension of the compliance date to ensure adequate time to implement the capability standards. This compliance date extension satisfies the second "C".

The third "C" -- cost recovery -- is central to implementing CALEA. The Act provides that the necessary upgrades must be "reasonably achievable". Compliance with CALEA, however, simply is not reasonably achievable without a standard in place. Furthermore, such a situation would dramatically increase the cost to the government and industry since non-standard implementation would be an even more expensive proposition. Therefore, the January 1, 1995 cut off for upgrade reimbursement is, per se , unworkable.

CTIA proposes to solve the cost recovery problem by mutual agreement that compliance with CALEA is not reasonably achievable until standardized solutions are commercially available to carriers. Under this approach, carriers will be deemed to be in compliance with CALEA for all equipment, facilities and services installed or deployed before standardized solutions are commercially available. Under CALEA, if law enforcement desired a carrier to upgrade to the standard, it would fund the modifications. Conversely, compliance with the Act post the commercial availability cut off would be at the carrier's expense. This approach -- should not increase the cost to the government if the "pay for the enhancement once" policy is pursued by the Department of Justice as appears to be the case. (i.e., since the government would make a one-time purchase of the necessary software upgrade for each switch type the number of switches covered is irrelevant).

Finally, we will wait for the final "C" -- capacity from the FBI with interest. We encourage a reasonable capacity assessment and that the FBI avoid further delay in publishing law enforcement needs.

CTIA took seriously Chairman Rogers' and Chairman McCollum's admonitions to get on with CALEA implementation. We have proposed a solution, not a continuation of the debate. We hope you concur. CTIA is proposing a path forward that might be characterized as the most important or fifth "C" -- compromise. We look forward to your earliest reply.

Very truly yours,

Thomas E. Wheeler